IN THE CLAIMS

Complete listing of the claims:

1. (Currently amended) A method of encrypting a set of data, the method comprising:

generating an original set of data;

generating a reference set of data;

encoding the reference set of data; and

combining the original set of data with the encoded reference set of data to generate an encrypted set of data;

wherein the encoding of the reference set of data comprises phase encoding the reference set of data; and

wherein the phase encoding of the reference set of data comprises introducing a random phase into the reference set of data.

2. (Canceled)

3. (Canceled)

4. (Currently amended) The method as set forth in Claim ~~3~~ 1 wherein the introducing of a random phase into the reference set of data comprises introducing a random phase into the reference set of data according to the equation:

$$U_R(x,y;\Delta\varphi_p) = A_R(x,y)\exp\left[i\left(\varphi_R(x,y) + \Delta\varphi_p\right)\right]$$

wherein $\varphi_R(x,y)$ is a random function, $\Delta\varphi_p$ is a phase shift between the original set of data and the reference set of data and $A_R(x,y)$ is the amplitude of the phase encoded reference set of data.

5. (Original) The method as set forth in Claim 1 wherein the encoding of the reference set of data comprises amplitude encoding the reference set of data.

6. (Original) The method as set forth in Claim 5 wherein the amplitude encoding of the reference set of data comprises introducing a random amplitude into the reference set of data.

7. (Original) The method as set forth in Claim 6 wherein the introducing of a random amplitude into the reference set of data comprises introducing a random amplitude into the reference set of data according to the equation:

$$U_R(x,y;\Delta\varphi_p) = A_R(x,y)\exp\left[i\left(\varphi_R(x,y)+\Delta\varphi_p\right)\right]$$

wherein $A_R(x,y)$ is a random function, $\Delta\varphi_p$ is a phase shift between the reference set of data and the original set of data and $\varphi_R(x,y)$ is the phase of the phase encoded reference set of data.

8. (Original) The method as set forth in Claim 1 further comprising introducing a phase shift between the original set of data and the reference set of data.

9. (Original) The method as set forth in Claim 1 further comprising recording the encrypted set of data.

10. (Original) The method as set forth in Claim 9 wherein the recording of the encrypted set of data comprises recording the encrypted set of data in a hologram.

11. (Original) The method as set forth in Claim 10 wherein the recording of the encrypted set of data in a hologram comprises recording the encrypted set of data in a hologram according to the equation:

$$I_p(x,y) = [A_H(x,y)]^2 + [A_R(x,y)]^2 + 2A_H(x,y)A_R(x,y)\cos[\phi_H(x,y) - \varphi_R(x,y) - \Delta\varphi_p]$$

wherein p is an integer,

$$\phi_E(x,y) = \phi_H(x,y) - \varphi_R(x,y)$$

is the encrypted phase,

$$A_E(x,y) = A_H(x,y)A_R(x,y)$$

is the encrypted amplitude, $\Delta\varphi_p$ is a phase shift between the reference set of data and the original set of data, $[A_H(x,y)]^2$ is the intensity of the original set of data and $[A_R(x,y)]^2$ is the intensity of the encoded reference set of data.

12. (Original) The method as set forth in Claim 1 wherein the original set of data comprises an optical image, a digitized image, a one dimensional set of data, a two dimensional set of data, a multi-dimensional set of data, an electrical signal or an optical signal.

13. (Original) The method as set forth in Claim 1 wherein the reference set of data comprises an optical image, a digitized image, a one dimensional set of data, a two dimensional set of data, a multi-dimensional set of data, an electrical signal or an optical signal.

14. (Currently amended) A method of encrypting and decrypting a set of data, the method comprising:

generating an original set of data;

generating a reference set of data;

encoding the reference set of data;

combining the original set of data with the encoded reference set of data to generate an encrypted set of data; and

decrypting the encrypted set of data;

wherein the encoding of the reference set of data comprises phase encoding the reference set of data; and

wherein the phase encoding of the reference set of data comprises introducing a random phase into the reference set of data.

15. (Canceled)

16. (Canceled)

17. (Currently amended) The method as set forth in Claim 14 ~~16~~ wherein the introducing of a random phase into the reference set of data comprises introducing a random phase into the reference set of data according to the equation:

$$U_R(x,y;\Delta\varphi_p) = A_R(x,y)\exp\left[i\left(\varphi_R(x,y)+\Delta\varphi_p\right)\right]$$

wherein $\varphi_R(x,y)$ is a random function, $\Delta\varphi_p$ is a phase shift between the original set of data and the reference set of data and $A_R(x,y)$ is the amplitude of the phase encoded reference set of data.

18. (Original) The method as set forth in Claim 14 wherein the encoding of the reference set of data comprises amplitude encoding the reference set of data.

19. (Original) The method as set forth in Claim 18 wherein the amplitude encoding of the reference set of data comprises introducing a random amplitude into the reference set of data.

20. (Original) The method as set forth in Claim 19 wherein the introducing of a random amplitude into the reference set of data comprises introducing a random amplitude into the reference set of data according to the equation:

$$U_R(x,y;\Delta\varphi_p) = A_R(x,y)\exp\left[i\left(\varphi_R(x,y) + \Delta\varphi_p\right)\right]$$

wherein $A_R(x,y)$ is a random function, $\Delta\varphi_p$ is a phase shift between the reference set of data and the original set of data and $\varphi_R(x,y)$ is the phase of the phase encoded reference set of data.

21. (Original) The method as set forth in Claim 14 further comprising introducing a phase shift between the original set of data and the reference set of data.

22. (Original) The method as set forth in Claim 14 further comprising recording the encrypted set of data.

23. (Original) The method as set forth in Claim 22 wherein the recording of the encrypted set of data comprises recording the encrypted set of data in a hologram.

24. (Original) The method as set forth in Claim 23 wherein the recording of the encrypted set of data in a hologram comprises recording the encrypted set of data in a hologram according to the equation:

$$I_p(x,y) = \left[A_H(x,y)\right]^2 + \left[A_R(x,y)\right]^2 + 2A_H(x,y)A_R(x,y)\cos\left[\phi_H(x,y) - \varphi_R(x,y) - \Delta\varphi_p\right]$$

wherein, p is an integer,

$$\phi_E(x,y) = \phi_H(x,y) - \varphi_R(x,y)$$

is the encrypted phase and

$$A_E(x,y) = A_H(x,y)A_R(x,y)$$

is the encrypted amplitude, $\Delta\varphi_p$ is a phase shift between the reference set of data and the original set of data, $\left[A_H(x,y)\right]^2$ is the intensity of the original set of data and $\left[A_R(x,y)\right]^2$ is the intensity of the encoded reference set of data.

25. (Original) The method as set forth in Claim 14 wherein the original set of data comprises an optical image, a digitized image, a one dimensional set of data, a two dimensional set of data, a multi-dimensional set of data, an electrical signal or an optical signal.

26. (Original) The method as set forth in Claim 14 wherein the reference set of data comprises an optical image, a digitized image, a one dimensional set of data, a two dimensional set of data, a multi-dimensional set of data, an electrical signal or an optical signal.

27. (Original) The method as set forth in Claim 14 wherein the decrypting of the encrypted set of data comprises generating a set of decryption keys by generating a set of intensity patterns, I'_p, of the combination of the reference beam and a phase shifted reference beam.

28. (Original) The method as set forth in Claim 27 wherein the generation of a set of decryption keys includes generating a phase key.

29. (Original) The method as set forth in Claim 28 wherein the generation of a phase key includes generating a phase key according to the equation

$$\phi_K(x,y) = \phi_C - \varphi_R(x,y)$$

wherein ϕ_C is a constant $\varphi_R(x,y)$ is a random function.

30. (Original) The method as set forth in Claim 27 wherein the generation of a set of decryption keys includes generating an amplitude key.

31. (Original) The method as set forth in Claim 30 wherein the generation of an amplitude key includes generating an amplitude key according to the equation

$$A_K(x,y) = A_C A_R(x,y)$$

wherein A_C is a constant $A_R(x,y)$ is a random function.

32. (Original) The method as set forth in Claim 29 further comprising generating a decrypted phase.

33. (Original) The method as set forth in Claim 32 wherein the generating of a decrypted phase comprises generating a decrypted phase according to the equation

$$\phi_D(x,y) = \phi_E(x,y) - \phi_K(x,y)$$

wherein $\phi_E(x,y)$ is the encrypted phase and $\phi_K(x,y)$ is the phase key.

34. (Original) The method as set forth in Claim 32 wherein the generating of a decrypted phase comprises generating a decrypted phase according to the equation

$$\phi_D(x,y) = \arctan\left[\frac{(I_4 - I_2)(I'_1 - I'_3) - (I_1 - I_3)(I'_4 - I'_2)}{(I_4 - I_2)(I'_4 - I'_2) - (I_1 - I_3)(I'_1 - I'_3)}\right]$$

wherein I_p are the encrypted set of data and I'_p are the decrypted set of data and p is an integer.

35. (Original) The method as set forth in Claim 31 further comprising generating a decrypted amplitude.

36. (Original) The method as set forth in Claim 35 wherein the generating of a decrypted amplitude comprises generating a decrypted amplitude according to the equation

$$A_D(x,y) = \begin{cases} \dfrac{A_E(x,y)}{A_K(x,y)}, & \text{if } A_K(x,y) \neq 0 \\ 0, & \text{otherwise} \end{cases}$$

wherein $A_E(x,y)$ is the encrypted amplitude and $A_K(x,y)$ is the amplitude key.

37. (Original) The method as set forth in Claim 35 wherein the generating of a decrypted amplitude comprises generating a decrypted amplitude according to the equation

$$A_D(x,y) = \left[\frac{(I_1 - I_3)^2 + (I_4 - I_2)^2}{(I'_1 - I'_3)^2 + (I'_4 - I'_2)^2}\right]^{1/2}$$

wherein I_p are the encrypted set of data and I'_p are the decrypted set of data and p is an integer.

38. (Original) The method as set forth in Claim 11 wherein said $\phi_E(x,y)$ is expressed as

$$\phi_E(x,y) = \arctan\left(\frac{I_4 - I_2}{I_1 - I_3}\right)$$

is the encrypted phase and said $A_E(x,y)$ is expressed as

$$A_E(x,y) = \frac{1}{4}\left[(I_1 - I_3)^2 + (I_4 - I_2)^2\right]^{1/2}$$

is the encrypted amplitude.

39. (Original) The method as set forth in Claim 24 wherein said $\phi_E(x,y)$ is expressed as

$$\phi_E(x,y) = \arctan\left(\frac{I_4 - I_2}{I_1 - I_3}\right)$$

is the encrypted phase and said $A_E(x,y)$ is expressed as

$$A_E(x,y) = \frac{1}{4}\left[(I_1 - I_3)^2 + (I_4 - I_2)^2\right]^{1/2}$$

is the encrypted amplitude.

40. (Original) The method as set forth on Claim 29 wherein said $\phi_K(x,y)$ is expressed as

$$\phi_K(x,y) = \arctan\left(\frac{I'_4 - I'_2}{I'_1 - I'_3}\right),$$

I'_p are the decrypted set of data and p is an integer.

41. (Original) The method as set forth in Claim 31 wherein said $A_K(x,y)$ is expressed as

$$A_K(x,y) = \frac{1}{4}\left[(I'_1 - I'_3)^2 + (I'_4 - I'_2)^2\right]^{1/2},$$

I'_p are the decrypted set of data and p is an integer.

42. (Original) The method as set forth in Claim 32 further comprising generating a decrypted hologram according to the equation

$$U_D(x,y) = A_D(x,y)\exp[i\phi_D(x,y)]$$

wherein $\phi_D(x,y)$ is the phase of the decrypted hologram.

43. (Original) The method as set forth in Claim 42 further comprising reconstructing the original set of data from the decrypted hologram.

44. (Original) The method as set forth in Claim 35 further comprising generating a decrypted hologram according to the equation

$$U_D(x,y) = A_D(x,y)\exp[i\phi_D(x,y)]$$

wherein $A_D(x,y)$ is the amplitude of the decrypted hologram.

45. (Original) The method as set forth in Claim 44 further comprising reconstructing the original set of data from the decrypted hologram.

46. (Original) The method as set forth in Claim 23 wherein the recording of the encrypted set of data in a hologram comprises recording the encrypted set of data in a digital hologram.

47. (Original) The method as set forth in Claim 46 further comprising reconstructing the original set of data from the decrypted digital hologram.

48. (Original) The method as set forth in Claim 47 wherein the reconstructing of the original set of data from the decrypted digital hologram comprises generating the discrete complex amplitude distribution of the reconstructed original set of data from the equation

$$U_O(m',n') = \exp\left[\frac{-i\pi}{\lambda d}\left(\Delta x'^2 m'^2 + \Delta y'^2 n'^2\right)\right]\sum_{m'=0}^{N_x-1}\sum_{n'=0}^{N_y-1}U_D(m,n)$$
$$\times \exp\left[\frac{-i\pi}{\lambda d}\left(\Delta x^2 m^2 + \Delta y^2 n^2\right)\right]\exp\left[-i2\pi\left(\frac{m'm}{N_x}+\frac{n'n}{N_y}\right)\right]$$

wherein $U_D(m,n)$ is the discrete amplitude distribution of the decrypted digital hologram, m and n are coordinates in the plane of the hologram, m' and n' are coordinates in the reconstruction plane, Δx is the horizontal resolution in the hologram plane, Δy is the vertical resolution in the hologram plane, $\Delta x'$ is the horizontal resolution in the reconstruction plane, $\Delta y'$ is vertical resolution in the reconstruction plane, N_x is the number of detector pixels in the x direction and N_y is the number of detector pixels in the y direction.

49. (Original) The method as set forth in Claim 46 further comprising reconstructing a segment of the original set of data from the decrypted digital hologram.

50. (Original) The method as set forth in Claim 49 wherein the reconstructing of a segment of the original set of data from the decrypted digital hologram comprises defining a subset, $rect\left(\frac{m-a_x}{b_x},\frac{n-a_y}{b_y}\right)$, of the decrypted digital hologram wherein a_x is x coordinate of the center of the segment of the original set of data, a_y is the y coordinate of the center of the segment of the original set of data b_x is the width of the segment of the original set of data in the x direction, b_y is the width of the segment of the original set of data in the y direction and m and n are coordinates in the plane of the hologram.

51. (Original) The method as set forth in Claim 50 further comprising defining a partial discrete amplitude distribution over the subset of the decrypted digital hologram according to the equation

$$U'_D(m,n;a_x,a_y)=U_D(m,n)rect\left(\frac{m-a_x}{b_x},\frac{n-a_y}{b_y}\right)$$

wherein $U_D(m,n)$ is the discrete amplitude distribution of the decrypted digital hologram.

52. (Original) The method as set forth in Claim 51 further comprising applying a phase factor, $\exp\left[i2\pi(a_x m+a_y n)\right]$, to the partial discrete amplitude distribution according to the equation

$$U'_D(m,n;a_x,a_y)=U_D(m,n)rect\left(\frac{m-a_x}{b_x},\frac{n-a_y}{b_y}\right)\exp\left[i2\pi(a_x m+a_y n)\right].$$

53. (Original) The method as set forth in Claim 52 further comprising generating the discrete complex amplitude distribution of the segment of the original set of data from the decrypted digital hologram according to the equation

$$U'_o(m',n';\alpha,\beta) = \exp\left[\frac{-i\pi}{\lambda d}\left(\Delta x'^2 m'^2 + \Delta y'^2 n'^2\right)\right]\sum_{m'=0}^{N_x-1}\sum_{n'=0}^{N_y-1} U'_D\left(m,n;\frac{\alpha d}{\Delta x},\frac{\beta d}{\Delta y}\right)$$
$$\times \exp\left[\frac{-i\pi}{\lambda d}\left(\Delta x^2 m^2 + \Delta y^2 n^2\right)\right]\exp\left[-i2\pi\left(\frac{m'm}{N_x}+\frac{n'n}{N_y}\right)\right].$$

54. (Original) The method as set forth in Claim 27 further comprising recording the set of decryption keys.

55. (Original) The method as set forth in Claim 54 wherein the recording of the set of decryption keys includes digitally recording the set of decryption keys.

56. (Original) The method as set forth in Claim 55 wherein the digitally recording of the set of decryption keys comprises storing the set of decryption keys in a computer-readable storage medium.

57. (Original) The method as set forth in Claim 22 wherein the recording of the encrypted set of data comprises storing the encrypted set of data in a computer-readable storage medium.

58. (Original) The method as set forth in Claim 57 further comprising transmitting the encrypted set of data to remote locations over a distributed computer network.

59. (Currently amended) A storage medium encoded with a set of data created by:

generating an original set of data;

generating a reference set of data;

encoding the reference set of data;

combining the original set of data with the encoded reference set of data to generate an encrypted set of data; and

storing the encrypted set of data;

wherein the encoding of the reference set of data comprises phase encoding the reference set of data; and

wherein the phase encoding of the reference set of data comprises introducing a random phase into the reference set of data.

60. (Canceled)

61. (Canceled)

62. (Currently amended) The storage medium as set forth in Claim 59 ~~61~~ wherein the introducing of a random phase into the reference set of data comprises introducing a random phase into the reference set of data according to the equation:

$$U_R(x,y;\Delta\varphi_p) = A_R(x,y)\exp\left[i\left(\varphi_R(x,y)+\Delta\varphi_p\right)\right]$$

wherein $\varphi_R(x,y)$ is a random function, $\Delta\varphi_p$ is a phase shift between the original set of data and the reference set of data and $A_R(x,y)$ is the amplitude of the phase encoded reference set of data.

63. (Original) The storage medium as set forth in Claim 59 wherein the encoding of the reference set of data comprises amplitude encoding the reference set of data.

64. (Original) The storage medium as set forth in Claim 63 wherein the amplitude encoding of the reference set of data comprises introducing a random amplitude into the reference set of data.

65. (Original) The storage medium as set forth in Claim 64 wherein the introducing of a random amplitude into the reference set of data comprises introducing a random amplitude into the reference set of data according to the equation:

$$U_R(x,y;\Delta\varphi_p) = A_R(x,y)\exp\left[i\left(\varphi_R(x,y) + \Delta\varphi_p\right)\right]$$

wherein $A_R(x,y)$ is a random function, $\Delta\varphi_p$ is a phase shift between the reference set of data and the original set of data and $\varphi_R(x,y)$ is the phase of the phase encoded reference set of data.

66. (Original) The storage medium as set forth in Claim 59 further comprising introducing a phase shift between the original set of data and the reference set of data.

67. (Original) The storage medium as set forth in Claim 59 further comprising recording the encrypted set of data.

68. (Original) The storage medium as set forth in Claim 67 wherein the recording of the encrypted set of data comprises recording the encrypted set of data in a hologram.

69. (Original) The storage medium as set forth in Claim 59 wherein the recording of the encrypted set of data in a hologram comprises recording the encrypted set of data in a hologram according to the equation:

$$I_p(x,y) = [A_H(x,y)]^2 + [A_R(x,y)]^2 + 2A_H(x,y)A_R(x,y)\cos[\phi_H(x,y) - \varphi_R(x,y) - \Delta\varphi_p]$$

wherein p is an integer,

$$\phi_E(x,y) = \phi_H(x,y) - \varphi_R(x,y)$$

is the encrypted phase,

$$A_E(x,y) = A_H(x,y)A_R(x,y)$$

is the encrypted amplitude, $\Delta\varphi_p$ is a phase shift between the reference set of data and the original set of data, $[A_H(x,y)]^2$ is the intensity of the original set of data and $[A_R(x,y)]^2$ is the intensity of the encoded reference set of data.

70. (Original) The storage medium as set forth in Claim 59 wherein the original set of data comprises an optical image, a digitized image, a one dimensional set of data, a two dimensional set of data, a multi-dimensional set of data, an electrical signal or an optical signal.

71. (Original) The storage medium as set forth in Claim 59 wherein the reference set of data comprises an optical image, a digitized image, a one dimensional set of data, a two dimensional set of data, a multi-dimensional set of data, an electrical signal or an optical signal.

72. (Currently amended) A method of encrypting a set of data, the method comprising:

generating an original set of data;

generating a reference set of data;

encoding the original set of data; and

combining the encoded original set of data with the reference set of data to generate an encrypted set of data;

wherein the encoding of the original set of data comprises phase encoding the original set of data; and

wherein the phase encoding of the original set of data comprises introducing a random phase into the original set of data.

73. (Canceled).

74. (Canceled).

75. (Currently amended) The method as set forth in Claim 72 ~~74~~ wherein the introducing of a random phase into the original set of data comprises introducing a random phase into the original set of data according to the equation:

$$U_R(x,y;\Delta\varphi_p) = A_R(x,y)\exp\left[i\left(\varphi_R(x,y)+\Delta\varphi_p\right)\right]$$

wherein $\varphi_R(x,y)$ is a random function, $\Delta\varphi_p$ is a phase shift between the original set of data and the reference set of data and $A_R(x,y)$ is the amplitude of the phase encoded original set of data.

76. (Original) The method as set forth in Claim 72 wherein the encoding of the original set of data comprises amplitude encoding the original set of data.

77. (Original) The method as set forth in Claim 76 wherein the amplitude encoding of the original set of data comprises introducing a random amplitude into the original set of data.

78. (Original) The method as set forth in Claim 77 wherein the introducing of a random amplitude into the original set of data comprises introducing a random amplitude into the original set of data according to the equation:

$$U_R(x,y;\Delta\varphi_p) = A_R(x,y)\exp\left[i\left(\varphi_R(x,y)+\Delta\varphi_p\right)\right]$$

wherein $A_R(x,y)$ is a random function, $\Delta\varphi_p$ is a phase shift between the reference set of data and the original set of data and $\varphi_R(x,y)$ is the phase of the phase encoded original set of data.

79. (Original) The method as set forth in Claim 72 further comprising introducing a phase shift between the original set of data and the reference set of data.

80. (Original) The method as set forth in Claim 72 further comprising recording the encrypted set of data.

81. (Original) The method as set forth in Claim 80 wherein the recording of the encrypted set of data comprises recording the encrypted set of data in a hologram.

82. (Original)The method as set forth in Claim 81 wherein the recording of the encrypted set of data in a hologram comprises recording the encrypted set of data in a hologram according to the equation:

$$I_p(x,y) = \left[A_H(x,y)\right]^2 + \left[A_R(x,y)\right]^2 + 2A_H(x,y)A_R(x,y)\cos\left[\phi_H(x,y) - \varphi_R(x,y) - \Delta\varphi_p\right]$$

wherein p is an integer,

$$\phi_E(x,y) = \phi_H(x,y) - \varphi_R(x,y)$$

is the encrypted phase,

$$A_E(x,y) = A_H(x,y)A_R(x,y)$$

is the encrypted amplitude, $\Delta\varphi_p$ is a phase shift between the reference set of data and the original set of data, $\left[A_H(x,y)\right]^2$ is the intensity of the original set of data and $\left[A_R(x,y)\right]^2$ is the intensity of the encoded reference set of data.

83. (Original) The method as set forth in Claim 72 wherein the original set of data comprises an optical image, a digitized image, a one dimensional set of data, a two dimensional set of data, a multi-dimensional set of data, an electrical signal or an optical signal.

84. (Original) The method as set forth in Claim 72 wherein the reference set of data comprises an optical image, a digitized image, a one dimensional set of data, a two dimensional set of data, a multi-dimensional set of data, an electrical signal or an optical signal.

85-87 (Canceled)

88. (Original) The method as set forth in Claim 10 further comprising:

processing the encrypted set of data by compression of the hologram; and

conveying the compressed hologram to remote locations over a distributed computer network.

89. (Original) The method as set forth in Claim 23 further comprising:

processing the encrypted set of data by compression of the hologram; and

conveying the compressed hologram to remote locations over a distributed computer network.

90. (Original) The method as set forth in Claim 81 further comprising:

processing the encrypted set of data by compression of the hologram; and

conveying the compressed hologram to remote locations over a distributed computer network.

91-112 (canceled)

113. (Original) The method as set forth in Claim 47 wherein reconstructing the original set of data from the decrypted digital hologram comprises reconstructing the original set of data by digital image processing.

114. (Original) The method as set forth in Claim 47 wherein reconstructing the original set of data from the decrypted digital hologram comprises reconstructing the original set of data by optical image processing.

115-142 canceled.

143. (New) A method of encrypting and decrypting a set of data, the method comprising:

generating an original set of data;

generating a reference set of data;

encoding the reference set of data;

combining the original set of data with the encoded reference set of data to generate an encrypted set of data; and

decrypting the encrypted set of data;

wherein the decrypting of the encrypted set of data comprises generating a set of decryption keys by generating a set of intensity patterns, I'_p, of the combination of a reference beam and a phase shifted reference beam;

wherein the generation of a set of decryption keys includes generating a phase key; and

wherein the generation of a phase key includes generating a phase key according to the equation:

$$\phi_K(x,y) = \phi_C - \varphi_R(x,y)$$

wherein ϕ_C is a constant $\varphi_R(x,y)$ is a random function.

144. (New) The method as set forth in Claim 143 wherein said $\phi_K(x,y)$ is expressed as

$$\phi_K(x,y) = \arctan\left(\frac{I'_4 - I'_2}{I'_1 - I'_3}\right),$$

I'_p are the decrypted set of data and p is an integer.

145. (New) The method as set forth in Claim 143 further comprising generating a decrypted phase.

146. (New) The method as set forth in Claim 145 wherein the generating of a decrypted phase comprises generating a decrypted phase according to the equation:

$$\phi_D(x,y) = \phi_E(x,y) - \phi_K(x,y)$$

wherein $\phi_E(x,y)$ is the encrypted phase and $\phi_K(x,y)$ is the phase key.

147. (New) The method as set forth in Claim 145 wherein the generating of a decrypted phase comprises generating a decrypted phase according to the equation

$$\phi_D(x,y) = \arctan\left[\frac{(I_4 - I_2)(I'_1 - I'_3) - (I_1 - I_3)(I'_4 - I'_2)}{(I_4 - I_2)(I'_4 - I'_2) - (I_1 - I_3)(I'_1 - I'_3)}\right]$$

wherein I_p are the encrypted set of data and I'_p are the decrypted set of data and p is an integer.

148. (New) The method as set forth in Claim 145 further comprising generating a decrypted hologram according to the equation

$$U_D(x,y) = A_D(x,y)\exp[i\phi_D(x,y)]$$

wherein $\phi_D(x,y)$ is the phase of the decrypted hologram.

149. (New) The method as set forth in Claim 148 further comprising reconstructing the original set of data from the decrypted hologram.

150. (New) A method of encrypting and decrypting a set of data, the method comprising:

generating an original set of data;

generating a reference set of data;

encoding the reference set of data;

combining the original set of data with the encoded reference set of data to generate an encrypted set of data; and

decrypting the encrypted set of data;

wherein the decrypting of the encrypted set of data comprises generating a set of decryption keys by generating a set of intensity patterns, I'_p, of the combination of a reference beam and a phase shifted reference beam;

wherein the generation of a set of decryption keys includes generating an amplitude key; and

wherein the generation of an amplitude key includes generating an amplitude key according to the equation:

$$A_K(x,y) = A_C A_R(x,y)$$

wherein A_C is a constant $A_R(x,y)$ is a random function.

151. (New) The method as set forth in Claim 150 wherein said $A_K(x,y)$ is expressed as

$$A_K(x,y) = \frac{1}{4}\left[(I'_1 - I'_3)^2 + (I'_4 - I'_2)^2\right]^{1/2}, \text{ where}$$

I'_p are the decrypted set of data and p is an integer.

152. (New) The method as set forth in Claim 150 further comprising generating a decrypted amplitude.

153. (New) The method as set forth in Claim 152 wherein the generating of a decrypted amplitude comprises generating a decrypted amplitude according to the equation

$$A_D(x,y) = \begin{cases} \dfrac{A_E(x,y)}{A_K(x,y)}, & \text{if } A_K(x,y) \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

wherein $A_E(x,y)$ is the encrypted amplitude and $A_K(x,y)$ is the amplitude key.

154. (New) The method as set forth in Claim 152 wherein the generating of a decrypted amplitude comprises generating a decrypted amplitude according to the equation

$$A_D(x,y) = \left[\frac{(I_1 - I_3)^2 + (I_4 - I_2)^2}{(I'_1 - I'_3)^2 + (I'_4 - I'_2)^2} \right]^{1/2}$$

wherein I_p are the encrypted set of data and I'_p are the decrypted set of data and p is an integer.

155. (New) The method as set forth in Claim 152 further comprising generating a decrypted hologram according to the equation:

$$U_D(x,y) = A_D(x,y) \exp[i\phi_D(x,y)]$$

wherein $A_D(x,y)$ is the amplitude of the decrypted hologram.

156. (New) The method as set forth in Claim 155 further comprising reconstructing the original set of data from the decrypted hologram.

157. (New) A method of encrypting and decrypting a set of data, the method comprising:

generating an original set of data;

generating a reference set of data;

encoding the reference set of data;

combining the original set of data with the encoded reference set of data to generate an encrypted set of data; and

decrypting the encrypted set of data;

further comprising recording the encrypted set of data;

wherein the recording of the encrypted set of data comprises recording the encrypted set of data in a hologram;

wherein the recording of the encrypted set of data in a hologram comprises recording the encrypted set of data in a digital hologram;

further comprising reconstructing a segment of the original set of data from the decrypted digital hologram;

wherein the reconstructing of a segment of the original set of data from the decrypted digital hologram comprises defining a subset, $rect\left(\frac{m-a_x}{b_x},\frac{n-a_y}{b_y}\right)$, of the decrypted digital hologram wherein a_x is x coordinate of the center of the segment of the original set of data, a_y is the y coordinate of the center of the segment of the original set of data b_x is the width of the segment of the original set of data in the x direction, b_y is the width of the segment of the original set of data in the y direction and m and n are coordinates in the plane of the hologram.

158. (New) The method as set forth in Claim 157 further comprising defining a partial discrete amplitude distribution over the subset of the decrypted digital hologram according to the equation

$$U'_D(m,n;a_x,a_y) = U_D(m,n)rect\left(\frac{m-a_x}{b_x},\frac{n-a_y}{b_y}\right)$$

wherein $U_D(m,n)$ is the discrete amplitude distribution of the decrypted digital hologram.

159. (New) The method as set forth in Claim 157 further comprising applying a phase factor, $\exp\left[i2\pi(a_x m + a_y n)\right]$, to the partial discrete amplitude distribution according to the equation

$$U'_D(m,n;a_x,a_y) = U_D(m,n)rect\left(\frac{m-a_x}{b_x},\frac{n-a_y}{b_y}\right)\exp\left[i2\pi(a_x m + a_y n)\right].$$

160. (New) The method as set forth in Claim 159 further comprising generating the discrete complex amplitude distribution of the segment of the original set of data from the decrypted digital hologram according to the equation

$$U'_o(m',n';\alpha,\beta) = \exp\left[\frac{-i\pi}{\lambda d}\left(\Delta x'^2 m'^2 + \Delta y'^2 n'^2\right)\right]\sum_{m'=0}^{N_x-1}\sum_{n'=0}^{N_y-1} U'_D\left(m,n;\frac{\alpha d}{\Delta x},\frac{\beta d}{\Delta y}\right)$$
$$\times \exp\left[\frac{-i\pi}{\lambda d}\left(\Delta x^2 m^2 + \Delta y^2 n^2\right)\right]\exp\left[-i2\pi\left(\frac{m'm}{N_x}+\frac{n'n}{N_y}\right)\right]$$